Temporary Assumptions for Quantum Multiparty Secure Computations

J. Müller-Quade and H. Imai

Imai Laboratory, Institute of Industrial Science, The University of Tokyo

(May 31st, 2001)

This paper introduces quantum multiparty protocols which allow the use of temporary assumptions. We prove that secure quantum multiparty computations are possible if and only if classical multi party computations work. But these strict assumptions are necessary only during the execution of the protocol and can be loosened after termination of the protocol.

We consider two settings:

1. A collusion of players tries to learn the secret inputs of honest players or tries to modify the result of the computation.

2. A collusion of players cheats in the above way or tries to disrupt the protocol, i. e., the collusion tries to abort the computation or leaks information to honest players.

We give bounds on the collusions tolerable after a protocol has terminated and we state protocols reaching these bounds.

03.67.-a, 03.67.Dd, 89.70.+c

I. INTRODUCTION

Due
to the no-go theorems of Mayers and Lo/Chau [28,24] and Lo [23] quantum cryptography cannot—with unconditional security—implement bit commitment, oblivious transfer and many other important two party protocols.

Here we give an analysis of the case of multiparty protocols.

We will investigate two settings. First multiparty protocols which we call *partially robust*, which can tolerate all forms of cheating, but can be aborted by a collusion of disruptors and secondly we will consider multiparty protocols which are *robust* even against disruption [29].

In the case without disruption classical multiparty protocols can yield unconditional security against all possible forms of cheating if a majority of the players is honest and one assumes private channels between any two parties as well as a broadcast channel [2,10,32]. More general for every set of possibly colluding parties secure multiparty computations are possible if no two collusions cover the total set of players [16].

From the no-go theorems for quantum two party protocols it can be concluded that there exist functions which cannot be realized by secure quantum multiparty protocols if two sets of possibly colluding parties cover the complete set of players. If the possible collusions are only defined by their cardinality multiparty protocols using

quantum cryptography become insecure if not a majority of players behave honestly.

Still quantum multiparty protocols have advantages over classical multiparty protocols. In this paper we prove that the assumptions about possible collusions can be loosened after the execution of the protocol. We present protocols where a majority may become dishonest after the protocol has terminated. Furthermore we give a limit on the collusions which are tolerable after the execution of the protocol. These bounds depend on the collusions which are tolerable during the execution of the protocol.

In the case with disruption we need that no two possible collusions cover all but one players, i. e., the cardinality of the union of two collusions never reaches $n-1$ for $|P| = n$. Given this assumption we can again prove that the assumptions about possible collusions can be loosened after the execution of the protocol. We also give limits on the collusions which are tolerable after the execution of the protocol and prove that these limits are tight.

We will restrict our view mostly to realizing a bit commitment from one party (called Alice) to a party named Bob. For our impossibility results we simply prove that relative to the given assumptions there cannot exist a multiparty protocol realizing a bit commitment from Alice to Bob. This implies that under the given assumptions there exist functions which cannot be computed securely. For the constructive results it is again enough to look at bit commiment, because with a result of Yao [34] we can realize an oblivious transfer channel using a quantum channel and bit commitments. With such an oblivious transfer channel between every pair of players we can realize multiparty computations, even with a dishonest majority [1,14,13,29]. Our concern will hence be to characterize the assumptions relative to which a bit commitment between two of the players becomes possible.

The structure of the paper is as follows. In Section II we will review definitions and known results on classical multiparty protocols and secret sharing techniques as far as we need them to prove our results. Next, in Section III we review the impossiblity of quantum bit commitment in the two party scenario [28,24]. We give some generalizations to the situation of multiparty protocols. In Section IV we stress the cryptographic importance of assumptions which can be loosened after a limited time, so called *temporary assumptions*. Then in the Sections V,VI, VII we give protocols which allow temporary assumptions in secure multiparty computations. The main idea is to use a classical secret sharing scheme

as a bit commitment protocol to force honest measurements. We show that, after the honest measurements are performed, the assumptions about possible collusions can be loosened.

II. CLASSICAL MULTIPARTY PROTOCOLS AND SECRET SHARING

A. Classical Multiparty Computations

In a multiparty protocol a set P of players wants to correctly compute a function $f(a_1, \ldots, a_n)$ which depends on secret inputs of n players. Some players might collude to cheat in the protocol as to obtain information about secret inputs of the other players or to modify the result of the computation.

When we look at the infrastructure available for the players we are mainly interested in three settings. First, there are private and authenticated channels between every pair of players and each player has a broadcast channel, second, every pair of players is connected by an oblivious transfer channel and a broadcast channel is available for everyone, and third, which is the setting for the results of this paper, every two players are connected by a quantum channel and an insecure but authenticated classical channel plus every player has access to a broadcast channel.

In multiparty computations we have to make some assumptions about possible collusions. We model possible collusions by defining a set of collusions. Only one of these possible collusions is actually cheating. Within this set of colluding players the players share their input and take actions based on their common knowledge.

Definition 1 *An adversary structure is a monotone set $\mathcal{A} \subseteq 2^P$, i.e., for a subset S' of a set $S \subseteq P$ the property $S \in \mathcal{A}$ implies $S' \in \mathcal{A}$.*

The main properties of a multiparty protocol are:

1. A multiparty protocol is said to be $\mathcal{A}$-*secure* if no single collusion from $\mathcal{A}$ is able to obtain information about the secret inputs of other participants which cannot be derived from the result and the inputs of the colluding players.

2. A multiparty protocol is $\mathcal{A}$-*partially correct* if no party can let the protocol terminate with a wrong result.

3. A multiparty protocol is $\mathcal{A}$-*correct* whenever no single collusion from $\mathcal{A}$ can abort the protocol, modify its result, or deviate from the protocol in a way that an honest player obtains information about the secret inputs of another player which cannot be derived from the result and the input of this honest player.

4. A multiparty protocol is called $\mathcal{A}$-*fair* if no collusion from $\mathcal{A}$ can reconstruct the result of the multi party computation earlier then all honest participants together. No collusion should be able to run off with the result.

A multiparty protocol having the properties 1., 2. and 4. is called $\mathcal{A}$-*partially robust* and a protocol having all three above properties is called $\mathcal{A}$-*robust.*

Whenever we are only concerned with partially robust protocols we will abort the protocol whenever a player complains about another player. Only robust protocols must be able to cope with conflicts between players.

Note that we allow only one collusion from $\mathcal{A}$ to cheat. Furthermore active cheaters are always be considered to be passively cheating, too.

Sometimes one thinks of all players being equivalent in their trustability, then adversary structures are solely defined by the cardinality of the collusions. When referring to an adversary structure which contains all subsets of P with no more than t players we denote the above properties by $\binom{n}{t}$-secure, $\binom{n}{t}$-(partially) correct, $\binom{n}{t}$-fair, and $\binom{n}{t}$-robust[1].

B. Multiparty Computations with Private Channels

We will summarize next what can be achieved by classical multiparty computations when private channels are available between any two players as well as a broadcast channel. The next result is taken from [16].

Theorem 2 *Given a set P of players with a secure and authenticated channel between each pair of players together with a broadcast cannel, then every function can be computed by an $\mathcal{A}$-partially robust multiparty protocol if no two sets from $\mathcal{A}$ cover the complete set P of players.*

Remark 3 *There exist functions for which a multiparty protocol among players who have access to a broadcast channel and have secure and authenticated channels connecting every pair of players cannot be $\mathcal{A}$-robust if two collusions cover $P \setminus \{P_i\}$ for some player P_i.*

Proof: If the players of two possible collusions $A_1, A_2 \in \mathcal{A}$ covering $P \setminus \{P_i\}$ cannot cooperate then it is not clear for P_i which collusion is cheating. To continue with the protocol all messages between players who are complaining about each other have to be exchanged over the broadcast channel or over secure channels via P_i. Obviously P_i learns all secrets or the protocol must

---

[1]Sometimes the terms t-secure, t-(partially) correct, t-fair, and t-robust are used for $\binom{n}{t-1}$-secure, $\binom{n}{t-1}$-correct, $\binom{n}{t-1}$-fair, and $\binom{n}{t-1}$-robust

be aborted. In both cases the protocol is not $\mathcal{A}$-robust.
□

As a corollary we state the classic result from [2,10] which was generalized to the situation with broadcast channel in [32].

Corollary 4 *Given n players which have a secure and authenticated channel between each pair of players together with a broadcast cannel, then every function can be computed by a $\binom{n}{t}$-partially robust multiparty protocol if $t < n/2$, i.e., if a majority is honest.*

C. Secret Sharing

One important primitive of classical multiparty protocols is secret sharing which was introduced in [33,7]. The aim of a secret sharing scheme is to allow a dealer to distribute shares $s_1, s_2, \ldots, s_n$, which represent one secret value x, to a set P of players such that only certain authorized subsets of P can reconstruct the secret x whereas all other subsets of P can't get any information about x. Of course every subset of P containing an authorized set must also be authorized. This leads to the definition of an *access structure*.

Definition 5 *An access structure is a set $\mathcal{Z} \subseteq 2^P$ for which for subsets $S' \supseteq S$ of P the property $S \in \mathcal{Z}$ implies $S' \in \mathcal{Z}$.*

An acess structure is "dual" to an adversary structure. If $\mathcal{A}$ is an adversary structure then the set $\{A^c | A \in \mathcal{A}\}$ forms an access structure.

The first access structures which were studied were defined by the cardinality of their minimal authorized sets. Later secret sharing schemes were constructed for arbitrary access structures [18,3].

For our protocol it is especially important to be able to keep the dealer from deliberately handing out faulty shares. Shares which do not match the agreed on access structure.

This problem can be overcome by verifiable secret sharing [4,10,6,16] which allows a verifier (e.g. each individual player) to check if a share he received is a valid share.

As we will use it later we sketch a verifiable secret sharing scheme from [4] which can be used for every homomorphic secret sharing scheme. I.e., for every scheme where the secrets form an additive group and sharing is a group homomorphism.

Verifiable Secret Sharing(m)

1. Alice shares a secret m with access structure$\mathcal{Z}$.

2. `for` $j = 1$ `to` k `do`

   (a) Alice shares a random secret z with the access structure $\mathcal{Z}$.

   (b) The verifier tells Alice to either open z or $z \oplus m$.

   (c) Alice publishes the shares for z or $z \oplus m$.

   `od`

If no player complains about the shares Alice publishes and if the shares published were correct shares then the verifier is convinced that all honest players hold correct shares.

It is clear that the secret m is shared correctly if z is shared correctly and $z \oplus m$ is shared correctly. A dishonest dealer will be caught cheating with a probability of $\frac{1}{2}$ in every of the k iterations. Hence the probability to pass this test with an incorrectly shared secret is 2^{-k} and thus negligible in k.

D. Multiparty Computations with Oblivious Transfer

Given an oblivious transfer channel all secure two party computations become possible with unconditional security [22]. This result was generalized to allow multiparty computations with a dishonest majority [1,14,13]. One obvious problem with such protocols is that if a majority of players cannot run off with the secret, i.e., they cannot reconstruct the secret on their own, then a minority of players can abort the protocol. For this reason we defined a multiparty protocol to be $\mathcal{A}$-*partially correct* if no collusion from $\mathcal{A}$ can make the protocol terminate with a wrong result.

The result of [1,14,13] can then be stated as

Theorem 6 *Given an oblivious transfer channel between any two players as well as a broadcast channel, then every function can be realized by a $\emptyset$-robust, 2^P-secure, 2^P-fair, and 2^P-partially correct multiparty protocol.*

In multiparty protocols the inputs are usually shared by a secret sharing scheme and the result is computed locally on the shares and by sharing intermediate results. In [1,14,13] the players are committed to the shares they hold. The computation in [13] uses a *global committed oblivious tranfer*, which is constructed there, to implement NOT and AND gates directly on the commitments. As the players are unable to cheat in the global committed oblivious tranfer and the players cannot open their commitments faultily every form of cheating is detectable. The only problem is that it is not always clear who is cheating. In [29] more robust protocols based on oblivious transfer were analyzed. There is a trade off between robustness and security as stated in the following result which are taken from [29].

Lemma 7 *Let P be a set of n players with every pair of players being connected by an oblivious transfer channel and every player having access to a broadcast channel.*

Let $\mathcal{A}$ and $\widetilde{\mathcal{A}}$ be adversary structures, then for all functions $\mathcal{A}$-robust and $\widetilde{\mathcal{A}}$-secure multiparty protocols exist if

1. the adversary structure $\mathcal{A}$ does not contain two sets covering $P \setminus \{P_i\}$ for any $P_i \in P$ and

2. the adversary structure $\widetilde{\mathcal{A}}$ contains only the complement of one previously chosen set B which is maximal in $\mathcal{A}$.

For a proof see [29]

In the above result one can see the trade off between robustness and security. The smaller $\mathcal{A}$ can be chosen the larger $\widetilde{\mathcal{A}}$ will be.

Corollary 8 *The protocol of Lemma 7 for the computation of a function $f(a_1, \ldots, a_n)$ is efficient in the number of players and the size of the circuit used to calculate $f(a_1, \ldots, a_n)$.*

For a proof see [29].

III. NO-GO RESULTS

A. Quantum Bit Commitment Is Impossible

In this section we will shortly review the impossibility of quantum bit commitment as proven by Mayers and Lo/Chau.

Definition 9 *A* bit commitment protocol *is a protocol consisting of two phases:* commit *and* unveil. *In the commit phase Bob obtains information from Alice which binds her to a certain bit b. In the unveil phase Alice opens b to Bob and proves to Bob that the commitment bound her to the bit b.*

A bit commitment protocol must have two properties:

1. binding, *i. e., after committing Alice can, without the help of Bob, only unveil one fixed bit b.*

2. concealing, *i. e., without the help of Alice Bob cannot know the bit b Alice committed to.*

To show the impossibility of quantum bit commitment one proceeds in two steps

1. First one shows that for each quantum protocol there exists a protocol which keeps all actions at the quantum level and postpones all measurements and random choices until shortly before unveil. This protocol is secure (binding and concealing) if and only if the original protocol was secure.

2. Then it is proven that (in the new protocol) either Bob can from his part of the quantum state distinguish between a comitted zero and a committed one (the protocol is not concealing) or Alice can with a quantum transformation change her part of

the quantum state from a superposition of commitments to zero into a superposition of commitments of one (and vice versa).

A key insight in the impossibility proofs given in [28,24] was that for each quantum protocol which involves measurements, random choices, and classical communication one can construct an equivalent protocol which has all measurements and random choices postponed to shortly before the unveil phase. With this reduction it is possible to treat the result of the commit phase as being a pure quantum state shared by Alice and Bob.

We will shortly explain the attack in more detail. Special emphasis is put on on classical communication during the protocol, as it involves measurements. But again these measurements can theoretically be delayed.

Alice behaves like she wants to honestly commit to zero and Bob behaves like an honest Bob, but all decisions which have to be made in the course of the protocol will no more be based on measurement results (or random choices), but will be done by *conditional quantum gates* [15] hence keeping all possibilities in superposition up to the measurement shortly before the unveil phase. Random choices are done in the same way, instead of fixing one value all possible values should be created in superposition. The most critical part of the reduction concerns classical communication. To get this classical data one must perform a measurement but even this measurement can be delayed to shortly before the unveil phase without changing the security of the protocol. Instead of measuring a qubit Alice entangles this qubit with two new qubits such that all three qubits give the same measurement result in the basis which should be used for the measurement (this is done by two *controlled not*) and sends one of these new qubits to Bob. This way Bob gets the information, and Alice can measure what information Bob got, but these measurements can be postponed without changing the security of the protocol.

If both parties follow this technique to keep everything at the quantum level, then the protocol will deliver, after the commit phase, a pure state shared by Alice and Bob.

This pure state $|\Psi_0\rangle$ appears on Alice side as a mixture $\rho_{Alice,0}$ (the index zero reminds us that Alice has committed to zero, the states $|\Psi_1\rangle$ and $\rho_{Alice,1}$ correspond to a commitment of one). On Bobs side the pure state appears as ρ_{Bob}.

Now we can import a result from [17].

Theorem 10 (Hughston, Jozsa, and Wootters)
Given two pure quantum states $|\psi\rangle$ and $|\phi\rangle$ shared between Alice and Bob which appear as the same state ρ on Bob's side, then there exists a unitary transform $U_{|\psi\rangle,|\phi\rangle}$ which acts on Alices part of the quantum system only and changes $|\psi\rangle$ to $|\phi\rangle$.

This result was generalized by Mayers to the case where $|\psi\rangle$ and $|\phi\rangle$ do not appear as the same state on Bob's side but as states which are very close to each other [26].

4

In the case of bit commitment this says that either the bit can be measured on Bob's side, i.e., ρ_{Bob} looks different for $|\Psi_0\rangle$ and $|\Psi_1\rangle$, or Alice can change from $|\Psi_0\rangle$ to $|\Psi_1\rangle$ by a unitary transform $\mathcal{U}_{0,1}$ on her part of the quantum system.

We can conclude the impossibility result from [28,24].

Theorem 11 (Mayers, Lo/Chau) *A quantum protocol for bit commitment cannot be binding and concealing.*

To cheat in the actual protocol it is of course not necessary that both parties keep their decisions at the quantum levels. It is enough if the party being able to cheat does so. See also Lemma 15.

B. Bounds on Tolerable Adversary Structures During the Execution of a Protocol

With the impossibility results for the two party case one can as well show that quantum cryptography cannot enhance classical bounds for the set of tolerable adversaries [16].

Corollary 12 *Let P be a set of players and let $\mathcal{A}$ be an adversary structure. If there exist two possible collusions $A_1, A_2 \in \mathcal{A}$ with $A_1 \cup A_2 = P$ then not all functions can be computed $\mathcal{A}$-partially robustly by a quantum multiparty protocol.*

Proof: We show that it is impossible to realize a bit commitment for a party Alice $\in A_1$ and Bob $\in A_2$. This is simple as we are almost in the two party scenario: Assume the collusion A_2 can by no means measure the bit Alice committed to, then the collusion A_1 can, by keeping every action at the quantum level cheat analogously to the two party situation, i.e., there exists a unitary transform $U_{0\rightarrow 1}$ which can change the bit Alice is committed to. The transform $U_{0\rightarrow 1}$ must be jointly applied by all players in A_1 □

Corollary 13 *There exist functions which cannot be computed $\binom{n}{t}$-partially robustly by a quantum multiparty protocol if $t \geq n/2$.*

If we consider robustness we have to take into account more deviations from the protocol. A collusion of players could for example leak their secret (quantum) data to a player not in the collusion. Such an attack further limits the set $\mathcal{A}$ of possible collusions.

Corollary 14 *Let P be a set of players and let $\mathcal{A}$ be an adversary structure. If there exist two possible collusions $A_1, A_2 \in \mathcal{A}$ with $A_1 \cup A_2 = P \setminus \{P_i\}$ for any player P_i, then not all functions can be computed $\mathcal{A}$-robustly by a quantum multiparty protocol.*

Proof: Assume there exists a $P_i \in P$ with $P = A_1 \cup A_2 \cup \{P_i\}$ for $A_1, A_2 \in \mathcal{A}$. We would like to implement a bit commitment from a player from A_2 to the player P_i. To prevent the players from A_2 to jointly change the committed bit it must be possible for the players of $A_1 \cup \{P_i\}$ to measure the committed bit. Only the assumption that P_i does not collude with the players of A_1 makes this attack impossible. If the player P_i is honest but curious and keeps everything at the quantum level, then he would be able to measure the committed bit if all players of the set A_1 would together keep all their actions at the quantum level and later on give all their quantum information to the player P_i.

Even though the player P_i does not collude with the players from A_1 we cannot keep the players from A_1 from deviating from the protocol in giving away their secret data. □

C. Bounds on Tolerable Adversary Structures After the Protocol Terminated

During the execution of a protocol we must use the same assumptions as in classical multiparty protocols to obtain unconditional security. We will next prove bounds on the set of tolerable collusions after a protocol has been finished. In our case: after the commit phase of a commitment protocol has terminated. Interestingly these bounds are different.

To apply the attack of Mayers and Lo/Chau Alice need not keep every action at the quantum level. She can perform measurements which yield not enough information to, together with the quantum information Bob has, be able to distinguish between the commitments zero and one. In short Alice can perform any measurement whose result she could tell Bob without giving away her secret commitment.

Lemma 15 *: Let $|\Psi_b\rangle$ be a pure quantum state shared between Alice and Bob which is the result of a quantum bit commitment protocol which was executed at the quantum level.*

If Alice can change the bit she committed to by a unitary transform $U_{0\rightarrow 1}$ on her part of $|\Psi_b\rangle$ then she can still change the bit after she performed a measurement on her part of the quantum state if the information obtained by this measurement together with the quantum information Bob holds does not allow to distinguish between the commitments zero and one.

Proof: One can define a bit commitment protocol where Alice has to perform this measurement and send the information measured to Bob. As Bob can still not distinguish between the commitments zero and one the attack of Mayers, Lo/Chau applies and there exists a unitary transform changing the bit. □

This simple result helps us to prove that temporarily having an honest but curious third party does not allow us to implement bit commitment [31].

Lemma 16 *Bit commitment may be implemented between Alice and Bob if we introduce a trusted third party, but the assumption of having an honest but curious third party is not a temporary assumption.*

Proof: If the honest but curious party remains independent of the two parties Alice and Bob bit commitment can be implemented by classical multiparty protocols.

Now assume the honest but curious third party joins Alice or Bob after the commit phase is completed.

The honest but curious third party will follow the protocol, but leave everything in superposition which need not be sent away as classical data. So the third party will perform some measurements. The third party can join Bob afterwards and Bob should still be unable to recover Alices bit. Hence the third party did only obtain measurement results which are of no use for Bob. Hence if the third party joins Alice we are in the situation of Lemma 15. Alice together with the third party can jointly perform a unitary transform which changes the bit Alice committed to. $\qquad\square$

Lemma 16 can be generalized to the multiparty scenario.

Proposition 17 *There exist functions for which no quantum multiparty protocol, which is partially robust against the adversary structure $\mathcal{A}$ can afterwards become secure against an adversary structure which contains two complements of sets in $\mathcal{A}$.*

Proof: Let $A_1, A_2 \in \mathcal{A}$ denote two sets of possibly colluding players and let $\widetilde{\mathcal{A}}$ be an adversary structure containing the complements of A_1 and A_2. We show that it is impossible to implement an oblivious transfer from Alice $\in A_1$ to Bob $\in A_2$ which is $\mathcal{A}$-partially robust and $\widetilde{\mathcal{A}}$-secure after termination. Assume such an oblivious transfer were possible then we could with it implement a bit commitment from Alice to Bob which is $\mathcal{A}$-partially robust during the commit phase and $\widetilde{\mathcal{A}}$-partially robust up to the unveil phase. This is easy to see as after termination of the commit phase security is the only critical issue. The data computed during the commit phase cannot be changed any more and fairness is not of interest until the unveil phase.

It remains to be proven that a bit commitment from the player Alice $\in A_1$ to the player Bob $\in A_2 \setminus A_1$ is impossible. We look at the sets A_1, $A_2 \setminus A_1$ and $P \setminus (A_1 \cup A_2)$ and prove the impossibility analogously to Lemma 16. During the execution of the commit phase the protocol is $\mathcal{A}$-partially robust hence we can assume that the players in A_1 or the players in $A_2 \setminus A_1$ collude and we still get a valid commitment from A_1 to $A_2 \setminus A_1$. Now we assume the protocol to become $\widetilde{\mathcal{A}}$-partially robust afterwards. Then all players from $P \setminus (A_1 \cup A_2)$ may join the players from $A_2 \setminus A_1$ and the bit commitment remains concealing even if the players from $A_2 \setminus A_1$ were colluding. Hence all quantum information in the posession of the players from $P \setminus (A_1 \cup A_2)$ are of no use to Bob. According to Lemma 15

the players from $A_1 \cup P \setminus (A_1 \cup A_2) = P \setminus A_2 = A_2^c$ can change the committed bit. Hence the bit commitment is not $\widetilde{\mathcal{A}}$-partially robust between commit and unveil. $\qquad\square$

Corollary 18 *There exist functions for which no $\binom{n}{t}$-robust quantum multiparty protocol can become $\binom{n}{n-t}$-robust after its execution.*

IV. TEMPORARY ASSUMPTIONS

Usually assumptions have to be made very carefully, because they implicitly try to predict future developements. The assumptions must be valid as long as the secret information is critical.

Temporary assumptions are hence very promising. There was little research into temporary assumptions in quantum cryptography after it became clear that computational assumptions cannot be used only temptorarily [9].

But quantum cryptography allows assumptions which are independent of computational assumptions. Such assumptions can be temporary.

The key idea to get temporary assumptions is to not try to make the transformation $\mathcal{U}_{0,1}$, which can change the committed bit, impossible, but to make it impossible for the parties (at least for the party able to cheat) to keep all actions at the quantum level.

E. g. Alice can trivially not cheat in the protocol of [5] if she has no quantum storage, even if quantum storage became available to her after the commit phase.

Assumptions which have the same effect are: limited quantum storage capacity and limited storage time for quantum bits as well as assumptions about decay introducing errors. Such assumptions need only hold during the execution of the protocol.

V. FORCING MEASUREMENTS WITH SECRET SHARING

In [34] Yao proved that it is possible to obtain oblivious transfer from a *black box* bit commitment and a quantum channel. The idea goes back to Crepeau [11] and was generalized to quantum channels which can have noise by Mayers [25].

The basic idea is to force measurements to avoid the attacks of Mayers and Lo/Chau and Lo [28,24,23]. In the course of the protocol one party has to commit to the measurment bases used and to the results obtained. Then a random subset of these measurments are opened. If there are not too many discrepancies one can be sure that the committing party did measure most of the qubits. This already suffices to make the delay of all measurements impossible hence avoiding the attacks of Mayers and Lo/Chau and Lo [34,25]. But one has to be careful if the bit commitment used is strong enough to force

measurements. The *unconditionally secure bit commitment* of Kent [21] is not suitable as Kent proved in [20].

The main requirement for a bit commitment to be able to force measurments is that committing to a bit b must be equivalent to giving the classical bit b to a trusted third party. Committing to a measurement result according to [34,25] implies an irreversible measurement as otherwise the cheater and the trusted third party together could violate the Heisenberg uncertainty.

In this section we will show that secret sharing can be used like a *black box* bit commitment to force measurements using the protocols of [34,25].

If we use, instead of bit commitment, secret sharing with an access structure $\mathcal{Z}$ and let $\mathcal{A}$ be the set $\{A|A^c \in \mathcal{Z}\}$ then we have the following properties:

1. the bit commitment based on secret sharing is concealing given only a collusion of $\{A|A \notin \mathcal{Z}\}$ is cheating.

2. The bit commitment based on secret sharing is binding if only one collusion of $\mathcal{A}$ is cheating.

3. The bit commitment based on secret sharing is equivalent to announcing the bit to a trusted third party whenever only one collusion of $\mathcal{A}$ is cheating.

The first two points of this enumeration follow directly from the properties of secret sharing schemes. Now we look at the third point. According to the assumption that only one collusion of $\mathcal{A}$ cheats we know that there exists a set M of honest players able to reconstruct the shared secret. As all players of M are honest the committing player (Alice) had to honestly transmit all the shares of the players of M. These shares already fix the committed bit and hence handing out those shares is equivalent to announcing the bit to a trusted third party. From this the next result follows without further proof.

Lemma 19 *Let $\mathcal{A}$ be an adversary structure and let $\mathcal{Z}$ be an access structure such that $\mathcal{A} = \{A|A^c \in \mathcal{Z}\}$. Then secret sharing with access structure $\mathcal{Z}$ can be used to obtain $\mathcal{A}$-partially robust oblivious transfer from any player to the dealer. The protocol is $\{A|A \notin \mathcal{Z}\}$-secure.*

After the measurements are irreversibly performed and the quantum attacks are impossible the bit commitment used need not be binding any more. Only the concealing property is still needed. For secret sharing the requirements for binding and concealing are different as seen in the enumeration above. So after all measurements are performed, especially after termination of the protocol, only collusions from $\{A|A \notin \mathcal{Z}\}$ can cheat in the oblivious transfer.

Of course we want oblivious transfer not only from one party to a set of players, but between every pair of players. The next section will give a detailed analysis of this situation.

VI. PARTIALLY ROBUST PROTOCOLS FOR OBLIVIOUS TRANSFER

We will next give a detailed analysis of the situation where we have a set P of players together with an adversary structure $\mathcal{A}$ and every player should be able to share a secret among the other players.

We are only concerned with partially robust protocols here. Whenever a player complains about another player we will abort the protocol. Robust protocols will be presented in the next section.

Lemma 20 *Let P be a set of players for which each pair of players is connected by an authenticated secure channel and every player has access to a broadcast channel. Let $\mathcal{A}$ be an adversary structure for which no two collusions cover the set P of players. Then a bit commitment between any pair of players is possible which is $\mathcal{A}$-partially robust and $\{A^c|A \notin \mathcal{A}\}$-secure.*

Proof: We will let Alice commit to a bit string $m \in \{0,1\}^k$.

Commit via Secret Sharing(m)

1. Alice sends Bob a random string $r \in \{0,1\}^k$.

2. Alice shares the string $m \oplus r$ using a secret sharing scheme with access structure $\mathcal{Z} = \{Z|Z^c \notin \mathcal{A}\}$.

This protocol shares Alices secret m with the access structure $\mathcal{Z} \cap \{M \subseteq P|\text{Bob} \in M\}$. If the receiver Bob is honest this protocol can be used to force measurements $\mathcal{A}$-partially robustly (Lemma 19) and if Bob is not honest then we cannot prevent a dishonest sender from colluding and changing the committed bit together with the receiver of the bit commitment. No bit commitment scheme can.

The unveil protocol is essentially a reconstruction of the shared secret.

Unveil

1. Alice announces the shares she sent. The players from P confirm the shares and Bob can then reconstruct m from his knowledge of r.

$\square$

We can improve the security a little bit further by not allowing every player to commit a bit via secret sharing. To obtain oblivious transfer between every pair of players it is enough that for every pair of players one of them can commit to the other as oblivious transfer can be inverted [12].

Lemma 21 *Let P be a set of players for which each pair of players is connected by an authenticated secure channel and every player has access to a broadcast channel. Let $\mathcal{A}$ be an adversary structure for which no two collusions cover the set P of players and let M be any maximal set*

in $\mathcal{A}$. Then for every pair of players a bit commitment is possible for one of the players to the other player which is $\mathcal{A}$-partially robust and $\{A^c|A \notin \mathcal{A}\} \cup M^c$-secure.

Proof: The partial robustness is the same as claimed by Lemma 20 so we need to prove only the improved security.

We have to see first that $\{A^c|A \notin \mathcal{A}\} \cup M^c$ is an adversary structure. The set $\{A^c|A \notin \mathcal{A}\}$ is an adversary structure and it contains all proper subsets of M^c. Hence the set $\{A^c|A \notin \mathcal{A}\} \cup M^c$ is an adversary structure, too.

To obtain the higher security we choose for every pair of players one player who shall commit to the other. Let Alice and Bob be a pair of players for which either Alice, Bob$\in M$, Alice, Bob$\notin M$ or Alice$\in M$ and Bob$\notin M$. Otherwise exchange the names of the players.

We will see that the bit commitment from Lemma 20 between any two players Alice and Bob is $\{A^c|A \notin \mathcal{A}\} \cup M^c$-secure if used in the above defined direction. As Lemma 20 already proves the $\{A^c|A \notin \mathcal{A}\}$-security we are left with proving the security against the possible collusion M^c.

A collusion can only cheat if it is an authorized set able to recover a shared secret and if it contains the receiver of the bit commitment as the shared secret is encrypted by a key r only known to the sender and the receiver of the bit commitment. If the collusion contains the sender of the bit commitment then the committed bit can already be derived from the inputs of the colluding players and no security is lost.

The direction of the bit commitment is chosen in a way that M^c either contains the sender of the bit commitment or it does not contain the receiver of the bit commitment and hence M^c is not able to reconstruct a secret bit in the bit commitment protocol. $\square$

From Lemma 19, Lemma 21 , and [12] we get the following result about oblivious transfer.

Corollary 22 *Let P be a set of players for which each pair of players is connected by an authenticated secure channel and every player has access to a broadcast channel. Let $\mathcal{A}$ be an adversary structure for which no two collusions cover the set P of players and let M be any maximal set in $\mathcal{A}$. Then an oblivious transfer is possible between every pair of players which is $\mathcal{A}$-partially robust and $\{A^c|A \notin \mathcal{A}\} \cup M^c$-secure.*

VII. ROBUST PROTOCOLS FOR OBLIVIOUS TRANSFER

In this section we will additionally consider players who try to disrupt the bit commitment protocol. In addition to the forms of cheating partially robust protocols can cope with we have that some players can leak out information to players not contained in their collusion or some players can claim that some other players do not follow

the protocol or they can themselves refuse to send or to receive messages.

If one looks at a secret sharing scheme step by step the only deviations of the protocol possible, which do not immediately give away the identity of the disruptor, are:

1. Some players might not keep their shares secret.

2. Some players complain that the sender presents different shares in the reconstruction phase then these players originally received.

3. Some players can claim to not receive any proper shares, e. g. empty shares.

This enumeration remains complete even if we consider verifiable secret sharing as we essentially iterate secret sharing together with some local computations (see Subsection II C).

If a disruption yields that the sender and the receiver of a bit commitment are in conflict then we will abort this bit commitment. We will not yet realize bit commitments between players who are in conflict with each other. We will later use multiparty protocols to obtain bit commitment and oblivious transfer between players who are in conflict.

Next we will give a bit commitment scheme based on verifiable secret sharing which can cope with disruption. Shares of complaining players will be published, but we will see that this does not harm the security. Thye number k is a security parameter.

Commit via Secret Sharing(m)

1. Alice shares the secret $m \oplus r$ with the access structure $\mathcal{Z}$ and sends r to Bob.

2. A set A complains about the shares they receive. These shares will be published by Alice

3. $A_{old} := A$

4. `repeat`

    (a) `for` $j = 1$ `to` k `do`

        i. Alice shares a random secret z with the access structure $\mathcal{Z}$.

        ii. Bob tells Alice to either open z or $z \oplus m \oplus r$.

        iii. Alice publishes the shares for z or $z \oplus m \oplus r$. A set A_j of players complains about these shares.

        iv. $A := A \cup A_j$

    `od`

    (b) If $A \notin \mathcal{A}$ then Alice is detected cheating else Alice has to publish the shares for the secret $m \oplus r$ for all players in A.

5. **until** $A_{old} = A$.

Lemma 23 *Let P be a set of players and let $\mathcal{A}$ be an adversary structure for which no two collusions cover the set $P \setminus \{P_i\}$ for any player P_i and let M be any maximal set in $\mathcal{A}$. Then a secret which is shared among the players of P according to the above protocol with access structure $\mathcal{Z} = \{Z | Z^c \in \mathcal{A}\}$ remains to be $\{A^c | A \notin \mathcal{A}\} \cup M^c$-secure even if a collusion of $\mathcal{A}$ publishes their shares.*

Proof: The security of a bit commitment scheme is only relevant if the sender is honest. So we can assume throughout the proof that the secret is properly shared.

Because no two collusions of $\mathcal{A}$ cover $P \setminus \{P_i\}$ every set of the access structure $\mathcal{Z} = \{Z | Z^c \in \mathcal{A}\}$ contains at least two honest players. So even if all players of a collusion $A \in \mathcal{A}$ leak their shares the secret remains shared among at least two honest players and no single honest but curious player gets to know a secret. $\square$

Lemma 24 *Let P be a set of players for which each pair of players is connected by an authenticated secure channel and every player has access to a broadcast channel. Let $\mathcal{A}$ be an adversary structure for which no two collusions cover the set $P \setminus \{P_i\}$ for any player P_i and let M be any maximal set in $\mathcal{A}$. Then for every pair of players, who will not be in conflict after the protocol, a bit commitment is possible from one of the players to the other player which is $\mathcal{A}$-robust and $\{A^c | A \notin \mathcal{A}\} \cup M^c$-secure.*

Proof: We are proving our claim using the above protocol. Whenever the receiver of the bit commitment complains about the sender then we need not be able to implement a bit commitment hence in the following we analyse only conflicts between the sender of the bit commitment and players other than the receiver.

We consider two cases.

First: Alice is honest, then every complaint about Alice comes from a cheater and Alice publishes the share the cheater complained about. So every complain about an honest Alice is equivalent to a leak of the share of the cheating player and we have seen that this does not harm the security of the secret sharing (Lemma 23). The correctness of the secret sharing, which implies the binding property of the bit commitment, cannot be harmed by shares which become publicly known.

Second: Alice is dishonest. Then Bob must be honest or we cannot expect a bit commitment to work. All shares the public ones as well as the only privately known ones pass the verifiable secret sharing test whenever the protocol has terminated and Alice has not been detected cheating. Hence every honest player is convinced that if Bob is honest then the secret is properly shared. This follows directly from the properties of the verifiable secret sharing scheme of [4] which was sketched in Subsection II C. The security of the protocol is not an issue if Alice is dishonest. $\square$

From the same arguments as used in Lemma 19 it is clear that the above bit commitment can be used to force measurements. As the direction of an oblivious transfer can be inverted [12] the directions of the bit commitments do not matter any more. Hence we can conclude the following.

Corollary 25 *Let P be a set of players for which each pair of players is connected by a quantum channel and an authenticated insecure channel and every player has access to a broadcast channel. Let $\mathcal{A}$ be an adversary structure for which no two collusions cover the set $P \setminus \{P_i\}$ for any player P_i and let M be any maximal set in $\mathcal{A}$. Then for every pair of players, who will not be in conflict after the protocol, an oblivious transfer is possible which is $\mathcal{A}$-robust and $\{A^c | A \notin \mathcal{A}\} \cup M^c$-secure.*

In the next section we will use the oblivious transfer of this corollary to implement multiparty computations.

A. Main Results

This section is separated in two subsections the first considering only partially robust protocols, i. e., protocols which are aborted whenever a conflict occurs and the second subsection deals with robust protocols tolerating every form of cheating and disruption.

B. Partially Robust Protocols

Combining the results of Corollary 12, Corollary 22, and [13] we get the following result without further proof.

Theorem 26 *Let P be a set of players each having access to a broadcast channel and let every pair of players of P be connected by a quantum channel and an insecure but authenticated classical channel. Then $\mathcal{A}$-partially robust quantum multiparty protocols for all functions exist if and only if no two collusions of $\mathcal{A}$ cover P.*

These protocols are $\widetilde{\mathcal{A}}$-secure after termination if and only if the adversary structure $\widetilde{\mathcal{A}}$ contains at most one complement of a previously chosen set from $\mathcal{A}$.

Secret sharing need not be efficient, but all other protocols used require only polynomial resources.

Corollary 27 *If secret sharing can be implemented efficiently for the access structure $\mathcal{Z} = \{A^c | A \in \mathcal{A}\}$ then the protocols of Theorem 26 can be efficient.*

C. Robust Protocols

To obtain robust protocols we must according to Lemma 14 choose $\mathcal{A}$ such that no two possible collusions together contain all but one players. In this situation we can use Lemma 7 together with Corollary 25 and obtain the following result without further proof.

Theorem 28 *Let P be a set of players each having access to a broadcast channel and every pair of players of P being connected by a quantum channel and an insecure but authenticated classical channel. Then $\mathcal{A}$-robust quantum multiparty protocols for all functions exist if and only if no two collusions of $\mathcal{A}$ cover $P \setminus \{P_i\}$ for any player P_i.*

These protocols are $\widetilde{\mathcal{A}}$-secure after termination if and only if the adversary structure $\widetilde{\mathcal{A}}$ contains at most one complement of a previously chosen set from $\mathcal{A}$.

If we are interested in robustness after termination and not security after termination we can use the following result from [29] (for a proof see [29]).

Lemma 29 *A multi party protocol which is $\mathcal{A}$-secure after termination is $\mathcal{B}$-robust after termination for $\mathcal{B} = \{B | \exists A \in \mathcal{A} : B \subset A \text{ and } B \neq A\}$.*

Again we need only polynomial resources if secret sharing is efficient.

Corollary 30 *If secret sharing can be implemented efficiently for the access structure $\mathcal{Z} = \{A^c | A \in \mathcal{A}\}$ then the protocols of Theorem 28 can be efficient.*

[1] D. Beaver and S. Goldwasser. Multiparty computations with faulty majority. In *Proceedings of the 30th FOCS*, pages 468–473. IEEE, 1989.

[2] M. Ben-Or, S. Goldwasser, and A. Widgerson. Completeness-theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th STOC*, pages 1–10. ACM, 1988.

[3] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology: Proceedings of Crypto '88*, volume 403 of *LNCS*, pages 27–36. Springer-Verlag, Berlin, 1990.

[4] J. Cohen Benaloh. Secret sharing homomorphisms: keeping shares of a secret secret. In A. M. Odlyzko, editor, *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *LNCS*, pages 251–260. Springer-Verlag, Berlin, 1986.

[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984.

[6] Th. Beth, H. Knobloch, and M. Otten. Verifiable secret sharing for monotone access structures. pages 189–194. ACM, Fairfax, USA, November 1993.

[7] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. AFIPS 1979*, volume 48, pages 313–317. NCC, Arlington, USA, June 1979.

[8] G. Brassard, C. Crepeau, D. Mayers, and L. Salvail. A brief review of the impossibility of quantum bit commitment. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9712023`, December 1997.

[9] G. Brassard, C. Crepeau, D. Mayers, and L. Salvail. Defeating classical bit commitments with a quantum computer. 1998. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9806031`.

[10] D. Chaum, C. Crepeau, and I. Damgaard. Multiparty unconditionally secure protocols. In *Proceedings of the 20th STOC*, pages 11–19. ACM, 1988.

[11] C. Crepeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, December 1994.

[12] C. Crepeau and M. Santha. On the reversibility of oblivious transfer. In *Advances in Cryptology: Proceedings of Eurocrypt '91*, volume 547 of *LNCS*, pages 106–113. Springer-Verlag, Berlin, 1991.

[13] C. Crepeau, J. van de Graaf, and A. Tapp. Committed oblivious transfer and private multi-party computations. In *Advances in Cryptology: Proceedings of Crypto '95*, pages 110–123. Springer, 1995.

[14] S. Goldwasser and L. Levin. Fair computation of general functions in presence of immoral majority. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology: Crypto '90*, volume 537 of *LNCS*, pages 77–93. Springer-Verlag, Berlin, 1990.

[15] J. Gruska. *Quantum Computing*. Advanced Topics in Computer Science. Mc Graw Hill, 1999.

[16] Martin Hirt and Ueli Maurer. Complete characterization of adversaries tolerable in secure multi-party computation. In *Proc. 16th ACM Symposium on Principles of Distributed Computing (PODC)*, pages 25–34, 1997.

[17] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a give density matrix. *Physics Letters A*, 183:14–18, 1993.

[18] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structures. In *Proc. Glob. Com.* 1987.

[19] A. Kent. Secure classical bit commitment over finite channels. 1999. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9906103`.

[20] A. Kent. Unconditional secure commitment of a certified classical bit is impossible. 1999. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9910087`.

[21] A. Kent. Unconditionally secure bit commitment. *Phys. Rev. Letters*, 83:2656–2659, 1999. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9810068`, See also [19].

[22] J. Kilian. Founding cryptography on oblivious transfer. In *Proc. 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 20–31. ACM, Chicago, 1988.

[23] H.-K. Lo. Insecurity of quantum secure computations. Accepted for publication in Phys. Rev. A.

[24] H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? Available on the Los Alamos preprint archieve at `xxx.lanl.gov`, March 1996.

[25] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Proceedings of Crypto'96*, Lecture Notes in Computer Science. Springer Verlag, Santa Barbara, 1996.

[26] D. Mayers. The trouble with bit commitment. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9603015`, 1996.

[27] D. Mayers. Unconditionally secure quantum bit commitment is impossible. Available on the Los Alamos preprint archieve at `xxx.lanl.gov` as `quant-ph/9712023`, 1996. Reprinted in the appendix of [8], it is D. Mayers first version of [28].

[28] D. Mayers. Unconditionally secure bit commitment is impossible. *Phys. Rev. Letters*, 78:3414–3417, 1997. A previous version was published at PhysComp96 [27].

[29] J. Müller-Quade and H. Imai. More robust multiparty protocols with oblivious transfer. Technical Report of ISEC 11 Technical Meeting, Tokyo, also as Los Alamos preprint quant-ph/0101020, October 2000.

[30] J. Müller-Quade and H. Imai. Quantum cryptographic three party protocols. Los Alamos preprint quant-ph/0010111, October 2000.

[31] J. Müller-Quade and H. Imai. Quantum protocols with a trusted authority. In *Proceedings of the 23rd Symposium on Information Theory and Its Applications*, volume II, Aso, Kumamoto, Japan, October 2000. IEEE Information Theory Society, Japanese Chapter.

[32] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the 21th STOC*, pages 73–85. ACM, 1989.

[33] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[34] A. Yao. Security of quantum protocols against coherent measurements. In *Procedings of the 27th Symposium on the Theory of Computing*, pages 67–75. ACM, Las Vegas, June 1995.